

CLAIMS

What is claimed is:

- 1 1. A method, comprising:
2 in an operating system environment controlled by a single operating system kernel
3 instance, establishing a global zone and at least one non-global zone for
4 isolating processes from processes in other non-global zones;
5 receiving from a first process executing in association with the non-global zone a first
6 request to perform an operation;
7 in response to receiving the first request, determining whether performing the
8 requested operation enables the first process to obtain additional privileges for
9 which the first process is not authorized; and
10 denying the first request if the first process is enabled to obtain the additional
11 privileges.
- 1 2. The method of claim 1, wherein each non-global zone has a set of allowable
2 privileges for processes executing within the non-global zone.
- 1 3. The method of claim 2, wherein the operation comprises obtaining control of a
2 second process, and wherein determining whether performing the requested operation
3 enables the first process to obtain the additional privileges comprises:
4 determining if a zone identifier of the first process matches with a zone identifier of a
5 second process; and
6 if the zone identifiers do not match, determining if the first process is
7 associated with a non-global zone; and if so, denying the request;

8 otherwise, determining if the first process has a privilege to control processes
9 in other zones; and
10 if the first process does not have the privilege to control processes in
11 other zones, denying the request;
12 determining if a user identifier of the first process matches with a user identifier of a
13 second process; and
14 if the user identifiers do not match, determining if the first process has a
15 process owner privilege; and
16 if the first process does not have the process owner privilege, denying
17 the request;
18 determining if the first process has at least each of the privileges possessed by the
19 second process; and
20 if the first process does not have each of the privileges of the second process,
21 denying the request;
22 determining if the user identifier of the second process is a privileged user identifier;
23 and
24 if the second process does not have a privileged user identifier, permitting the
25 request;
26 determining if the first process is associated with the global zone; and
27 if the first process is a global zone process, then determining if the first
28 process has all privileges; and
29 if so, permitting the request; otherwise, denying the request;

30 otherwise, if the first process is associated with a non-global zone, then
31 determining if the first process has all privileges in the set of allowable
32 privileges for the non-global zone; and
33 if so, permitting the request; otherwise, denying the request.

1 4. The method of claim 3, wherein the privileged user identifier is 0.

1 5. The method of claim 2, wherein establishing a non-global zone for isolating processes
2 from processes in other non-global zones, comprises:
3 setting a privilege limit for the non-global zone, the privilege limit indicating the set
4 of allowable privileges for processes executing within the non-global zone.

1 6. The method of claim 5, wherein the privilege limit is represented as a bit mask passed
2 to the non-global zone when created, the method further comprising:
3 comparing privileges held by a process joining the non-global zone against the bit
4 mask; and
5 removing any privileges not in the bit mask from the process.

1 7. The method of claim 1, wherein performing the requested operation comprises
2 accessing an object, the method further comprising:
3 determining whether the first process has permission to access the object.

1 8. The method of claim 1, wherein the operation includes one of:

(un)mounting a file system, overriding file system permissions, binding to a privileged network port, and controlling other processes with different user identifiers.

9. The method of claim 2, wherein the operation comprises changing a user identifier associated with the first process, and wherein determining whether performing the requested operation enables the first process to obtain the additional privileges comprises:

determining if the request is to change the user identifier associated with the first process to a privileged user identifier, and if the first process has at least each of the privileges in the set of allowable privileges for the non-global zone; and if so, granting the request;

otherwise, determining if the first process has a privilege appropriate for the request; and,

if so, granting the request;

otherwise, denying the request.

10. The method of claim 1, further comprising:

receiving from a process executing in association with the global zone a request to perform an operation;

in response to receiving the request, determining whether performing the requested operation enables the process to obtain additional privileges for which the process is not authorized; and

denying the request if the process is enabled to obtain the additional privileges.

11. The method of claim 10, wherein the operation comprises obtaining control of a second process, and wherein determining whether performing the requested operation enables the process executing in association with the global zone to obtain the additional privileges comprises:

- determining if a zone identifier of the first process matches with a zone identifier of a second process; and
- if the zone identifiers do not match, determining if the first process is associated with a non-global zone; and if so, denying the request;
- otherwise, determining if the first process has a privilege to control processes in other zones; and
- if the first process does not have the privilege to control processes in other zones, denying the request;

determining if a user identifier of the first process matches with a user identifier of a second process; and

- if the user identifiers do not match, determining if the first process has a process owner privilege; and
- if the first process does not have the process owner privilege, denying the request;

determining if the first process has at least each of the privileges possessed by the second process; and

- if the first process does not have each of the privileges of the second process, denying the request;

23 determining if the user identifier of the second process is a privileged user identifier;
24 and
25 if the second process does not have a privileged user identifier, permitting the
26 request;
27 determining if the first process is associated with the global zone; and
28 if the first process is a global zone process, then determining if the first
29 process has all privileges; and
30 if so, permitting the request; otherwise, denying the request;
31 otherwise, if the first process is associated with a non-global zone, then
32 determining if the first process has all privileges in the set of allowable
33 privileges for the non-global zone; and
34 if so, permitting the request; otherwise, denying the request.

1 12. The method of claim 10, wherein the operation comprises changing a user identifier
2 associated with the process executing in association with the global zone, and
3 wherein determining whether performing the requested operation enables the process
4 executing in association with the global zone to obtain the additional privileges
5 comprises:
6 determining if the request is to change the user identifier associated with the process
7 executing in association with the global zone to a privileged user identifier,
8 and if the process executing in association with the global zone has all
9 privileges; and
10 if so, granting the request;

11 otherwise, determining if the process executing in association with the global zone
12 has a privilege appropriate for the request; and,
13 if so, granting the request;
14 otherwise, denying the request.

1 13. The method of claim 10, wherein the operation includes one of:
2 modifying all process privileges, writing to system administration file, opening device
3 holding kernel memory, modifying operating system code, accessing file
4 systems restricted to root user, setting the system clock, changing scheduling
5 priority of an executing process, reserving resources for an application,
6 directly accessing a network layer and loading kernel modules.

1 14. A computer readable medium, comprising instructions for causing one or more
2 processors to perform the steps of:
3 establishing a global zone and at least one non-global zone for isolating processes
4 from processes in other non-global zones in an operating system environment
5 controlled by a single operating system kernel instance;
6 receiving from a first process executing in association with the non-global zone a first
7 request to perform an operation;
8 in response to receiving the first request, determining whether performing the
9 requested operation enables the first process to obtain additional privileges for
10 which the first process is not authorized; and
11 denying the first request if the first process is enabled to obtain the additional
12 privileges.

1 15. The computer readable medium of claim 14, wherein each non-global zone has a set
2 of allowable privileges for processes executing within the non-global zone.

1 16. The computer readable medium of claim 15, wherein the operation comprises
2 obtaining control of a second process, and wherein determining whether performing
3 the requested operation enables the first process to obtain the additional privileges
4 comprises:
5 determining if a zone identifier of the first process matches with a zone identifier of a
6 second process; and
7 if the zone identifiers do not match, determining if the first process is
8 associated with a non-global zone; and if so, denying the request;
9 otherwise, determining if the first process has a privilege to control processes
10 in other zones; and
11 if the first process does not have the privilege to control processes in
12 other zones, denying the request;
13 determining if a user identifier of the first process matches with a user identifier of a
14 second process; and
15 if the user identifiers do not match, determining if the first process has a
16 process owner privilege; and
17 if the first process does not have the process owner privilege, denying
18 the request;
19 determining if the first process has at least each of the privileges possessed by the
20 second process; and

21 if the first process does not have each of the privileges of the second process,
22 denying the request;
23 determining if the user identifier of the second process is a privileged user identifier;
24 and
25 if the second process does not have a privileged user identifier, permitting the
26 request;
27 determining if the first process is associated with the global zone; and
28 if the first process is a global zone process, then determining if the first
29 process has all privileges; and
30 if so, permitting the request; otherwise, denying the request;
31 otherwise, if the first process is associated with a non-global zone, then
32 determining if the first process has all privileges in the set of allowable
33 privileges for the non-global zone; and
34 if so, permitting the request; otherwise, denying the request.

1 17. The computer readable medium of claim 16, wherein the privileged user identifier
2 is 0.

1 18. The computer readable medium of claim 15, wherein establishing a non-global zone
2 for isolating processes from processes in other non-global zones, comprises:
3 setting a privilege limit for the non-global zone, the privilege limit indicating the set
4 of allowable privileges for processes executing within the non-global zone.

1 19. The computer readable medium of claim 18, wherein the privilege limit is represented
2 as a bit mask passed to the non-global zone, the computer readable medium further
3 comprising instructions for causing one or more processors to perform the steps of:
4 comparing privileges held by a process joining the non-global zone against the bit
5 mask; and
6 removing any privileges not in the bit mask from the process.

1 20. The computer readable medium of claim 14, wherein performing the requested
2 operation comprises accessing an object, the computer readable medium further
3 comprises instructions for causing one or more processors to perform the step of:
4 determining whether the first process has permission to access the object.

1 21. The computer readable medium of claim 14, wherein the operation includes one of:
2 (un)mounting a file system, overriding file system permissions, binding to a
3 privileged network port, and controlling other processes with different user
4 identifiers.

1 22. The computer readable medium of claim 15, wherein the operation comprises
2 changing a user identifier associated with the first process, and wherein determining
3 whether performing the requested operation enables the first process to obtain the
4 additional privileges comprises instructions for causing one or more processors to
5 perform the steps of:

6 determining if the request is to change the user identifier associated with the first
7 process to a privileged user identifier, and if the first process has at least each
8 of the privileges in the set of allowable privileges for the non-global zone; and
9 if so, granting the request;
10 otherwise, determining if the first process has a privilege appropriate for the request;
11 and,
12 if so, granting the request;
13 otherwise, denying the request.

1 23. The computer readable medium of claim 14, further comprising instructions for
2 causing one or more processors to perform the steps of:
3 receiving from a process executing in association with the global zone a request to
4 perform an operation;
5 in response to receiving the request, determining whether performing the requested
6 operation enables the process in the global zone to obtain privileges in
7 addition to privileges associated with the process; and
8 denying the request if the process is enabled to obtain additional privileges outside of
9 privileges associated with the process.

1 24. The computer readable medium of claim 23, wherein the operation comprises
2 obtaining control of a second process, and wherein determining whether performing
3 the requested operation enables the process executing in association with the global
4 zone to obtain the additional privileges comprises instructions for causing one or
5 more processors to perform the steps of:

6 determining if a zone identifier of the first process matches with a zone identifier of a
7 second process; and
8 if the zone identifiers do not match, determining if the first process is
9 associated with a non-global zone; and if so, denying the request;
10 otherwise, determining if the first process has a privilege to control processes
11 in other zones; and
12 if the first process does not have the privilege to control processes in
13 other zones, denying the request;
14 determining if a user identifier of the first process matches with a user identifier of a
15 second process; and
16 if the user identifiers do not match, determining if the first process has a
17 process owner privilege; and
18 if the first process does not have the process owner privilege, denying
19 the request;
20 determining if the first process has at least each of the privileges possessed by the
21 second process; and
22 if the first process does not have each of the privileges of the second process,
23 denying the request;
24 determining if the user identifier of the second process is a privileged user identifier;
25 and
26 if the second process does not have a privileged user identifier, permitting the
27 request;
28 determining if the first process is associated with the global zone; and

29 if the first process is a global zone process, then determining if the first
30 process has all privileges; and
31 if so, permitting the request; otherwise, denying the request;
32 otherwise, if the first process is associated with a non-global zone, then
33 determining if the first process has all privileges in the set of allowable
34 privileges for the non-global zone; and
35 if so, permitting the request; otherwise, denying the request.

1 25. The computer readable medium of claim 23, wherein the operation comprises
2 changing a user identifier associated with the process executing in association with
3 the global zone, and wherein determining whether performing the requested operation
4 enables the process executing in association with the global zone to obtain the
5 additional privileges comprises instructions for causing one or more processors to
6 perform the steps of:
7 determining if the request is to change the user identifier associated with the process
8 executing in association with the global zone to a privileged user identifier,
9 and if the process executing in association with the global zone has all
10 privileges; and
11 if so, granting the request;
12 otherwise, determining if the process executing in association with the global zone
13 has a privilege appropriate for the request; and,
14 if so, granting the request;
15 otherwise, denying the request.

1 26. The computer readable medium of claim 23, wherein the operation includes one of:
2 modifying all process privileges, writing to system administration file, opening device
3 holding kernel memory, modifying operating system code, accessing file
4 systems restricted to root user, setting the system clock, changing scheduling
5 priority of an executing process, reserving resources for an application,
6 directly accessing a network layer and loading kernel modules.

1 27. An apparatus, comprising:
2 means for establishing a global zone and at least one non-global zone for isolating
3 processes from processes in other non-global zones in an operating system
4 environment controlled by a single operating system kernel instance;
5 means for receiving from a first process executing in association with the non-global
6 zone a first request to perform an operation;
7 means for determining in response to receiving the first request whether performing
8 the requested operation enables the first process to obtain additional privileges
9 for which the first process is not authorized; and
10 means for denying the first request if the first process is enabled to obtain the
11 additional privileges.